IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Attorney Docket No. **RP9-99-048**

In re Application of:	§
	§
CROMER ET AL.	§
	§
Serial No. **09/281,852**	§
	§
Filed: **31 MARCH 1999**	§
	§
For: **DATA PROCESSING SYSTEM**	§
AND METHOD FOR MAINTAINING	§
SECURE DATA BLOCKS	§

OFFICIAL

Examiner: **TRUONG, T.**

Art Unit: **2135**

APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief is submitted in triplicate in support of the Appeal in the above-identified application.

CERTIFICATE OF FACSIMILE
37 CFR § 1.8(a)

I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date below.

_8/19/04_
Date

Vicky Filipovsky
Signature

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, the real party of interest.

RELATED APPEALS AND INTERFERENCES

No related appeal is presently pending.

STATUS OF THE CLAIMS

Claims 1-7 and 10-16 stand finally rejected by the Examiner as noted in the Final Office Action dated May 21, 2004 and the Advisory Action dated August 3, 2004.

STATUS OF AMENDMENTS

No amendment was submitted subsequent to the Office Action dated February 27, 2004.

SUMMARY OF THE INVENTION

A website may send a block of data, commonly known as a *cookie*, to a user's computer system for the purpose of facilitating subsequent access to the website. The cookie may include public information pertaining to the website as well as private information associated with the user. With respect to a user's private information, a cookie may include, *inter alia*, a username along with a corresponding password, the user's credit card information, the user's address, and the user's online usage preferences. Because it is paramount to maintain the data security of cookies when private information are involved, it is most preferable to store cookies in a secure storage area of a user's computer system.

During each website access, a user's computer may receive cookies that need to be stored in a secure storage area of the user's computer system. Thus, over time, it is most likely that the number of cookies will eventually exceed the size of the secure storage area within the user's computer system. But if the "overflow" cookies are stored in a non-secured storage area of the user's computer system, such as a hard disk drive, it is foreseeable that an unauthorized user can copy a user's cookies from the user's computer system to another computer system for the

purpose of extracting valuable information stored within the cookies. Therefore, it is desirable to provide a method for storing cookies in a non-secured mass storage device within a user's computer system while without sacrificing the data security of the cookies.

In accordance with a preferred embodiment of the present invention, an encryption key pair, which includes a private key and a public key, is stored in a protected storage device within a data processing system, as shown in block **304** of Figure **3**. In response to the receipt of a cookie generated by an application from a remote server, the cookie is encrypted with the public key of the encryption key pair, as depicted in block **308** of Figure 3. The encrypted cookie can now be stored in a non-protected storage device, such as a hard disk drive, within the data processing system, as shown in block **310** of Figure 3. In response to an access request for the encrypted cookie by a browser program executing within the data processing system, a copy of the encrypted cookie is sent to the protected storage device, as depicted in block **408** of Figure **4**, and the encrypted cookie is decrypted using the private key within the protected storage device, as shown in block **410** of Figure **4**. Finally, the decrypted cookie is sent to the browser program requesting the cookie, as shown in block **412** of Figure **4**.

ISSUE

Is the Examiner's rejection of Claims 1-7 and 10-16 under 35 U.S.C. § 103(a) as being unpatentable over *Win et al.* (US 6,161,139) in view of *Shrader et al.* (US 6,374,359) well-founded?

GROUPING OF THE CLAIMS

For purposes of this Appeal, Claims 1-7 and 10-16 stand or fall together as a single group.

ARGUMENT

The Examiner's rejections of Claims 1-7 and 10-16 are not well-founded and should be reversed.

I.   The cited references do not teach or suggest a protected storage device for storing an encryption key pair and a non-protected storage device for storing encrypted cookies

The problem that the claimed invention intended to solve, as explained in the SUMMARY OF THE INVENTION section of the present appeal brief, is to provide a relatively inexpensive mass storage device within a data processing system for storing cookies while without sacrificing the data security of the cookies. The solution, as provided by the claimed invention, is to store cookies in a non-protected storage device because non-protected storage devices are typically less expensive than protected storage devices. In order to maintain data security, cookies are encrypted before storing in a non-protected storage device. Thus, Claim 1 (and similarly Claim 10) recites a step of "in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key" (lines 5-6) and a step of "storing said encrypted cookie in a non-protected storage device within said data processing system" (lines 7-8).

The above-mentioned public key is part of an encryption key pair that includes a private key and a public key. The encryption key pair is stored in a protected storage device within a data processing system for security reasons. Thus, Claim 1 recites a step of "storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system" (lines 3-4).

Hence, according to the claimed invention, an encryption key pair is stored in a protected storage device of a data processing system, and cookies are stored in a non-protected storage device of the data processing system after the cookies have been encrypted by a public key of the encryption key pair.

APPEAL BRIEF   PAGE 5   RP999048.BR3

On page 3 of the Final Office Action, the Examiner characterizes *Win*'s access server **106** as the claimed non-protected storage device, and on page 4 of the Final Office Action, the Examiner characterizes *Win*'s storage device **910** shown in Figure 9 as the claimed non-protected storage device. However, both of the above-mentioned characterizations are incorrect because neither access server **106** nor storage device **910** performs the functions of the claimed storage devices as recited in Claim 1. Thus, the Examiner has not clearly defined how the claimed non-protected storage device and the claimed protected storage device are being disclosed by *Win*.

In addition, on page 2 of the Final Office Action, the Examiner states that *Win* teaches that "the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a 'cookie' to the user's browser." Appellants agree with the Examiner that *Win* teaches the cookie being encrypted in Registry Server **108**. Since it is clear from Figure 1 of *Win* that Registry Server **108** is part of a secure intranet (col. 4, lines 33-34) and not part of a data processing system in which a browser resides, *Win* does not teach or suggest the cookie encryption being performed at the data processing system in which the browser resides, as claimed. *Shrader* does not teach or suggest the cookie encryption being performed at the data processing system in which the browser resides either. Because the claimed invention recites novel features that are not found in the cited references, whether considered separately or in combination, the § 103 rejection is improper.

On page 2 of the Advisory Action, the Examiner points to *Win*'s teachings of an alternative embodiment in which one or more components can be installed on separate computers. However, such teachings are irrelevant to the claimed invention because it is imperative for the claimed invention to have the encrypting step and the storing step to be performed within the same computer in which a browser resides and not on separate computers.

II.   The cited references do not teach or suggest a hard drive for storing encrypted cookies

An example of a non-protected storage device for storing cookies is a hard drive. Thus, Claim 2 (and similarly Claim 11) recites that "said non-protected storage device is a hard drive. (lines 1-2).

APPEAL BRIEF   PAGE 6   RP999048.BR3

On page 4 of the Final Office Action, the Examiner asserts that *Win* discloses the claimed non-protected storage device such as a storage device 910 shown in Figure 9. It is understood that most data processing systems includes non-protected storage devices such as hard drives. However, the claimed invention is not simply about whether or not a data processing system includes a non-protected storage device such as a hard disk, but rather, the claimed invention is related to the provision of using a non-protected storage device to store encrypted cookies. Claim 2 specifically recites one type of non-protected storage device, *i.e.*, a hard drive, to be used for storing encrypted cookies. In contrast, *Win* does not teach or suggest the use of storage device 910 for storing encrypted cookies. *Shrader* does not teach or suggest the usage of a non-protected storage device to store encrypted cookies either. Because the cited references, whether considered separately or in combination, do not teach or suggest the claimed invention, the § 103 rejection is improper.

III.   *Win* does not teach or suggest an encryption device having an encryption engine

Claim 3 (and similarly Claim 12) recites a step of "providing an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine" (lines 1-3).

On page 4 of the Final Office Action, the Examiner asserts that the claimed providing step is disclosed by *Win* but the Examiner has not specifically pointed to an entity in *Win* that can be considered as the claimed encryption device or its equivalent.

Furthermore, Claim 3 requires that the above-mentioned protected storage device can only be accessed through the claimed encryption engine. Since the Examiner has already stated that *Win* does not explicitly disclose the storage of an encryption key in a protected storage device, there would not be a reason for *Win* to include the claimed encryption engine. As such, *Win* does not teach or suggest the claimed providing step.

CONCLUSION

For the reasons stated above, Appellants believe that the claimed invention clearly is patentably distinct over the cited references and that the rejections under 35 U.S.C. § 103 are not well-founded. Hence, Appellants respectfully urge the Board to reverse the Examiner's rejection.

Please charge the IBM Deposit Account 50-0563 in the amount of $330.00 for submission of a Brief in support of Appeal. No fee or extension of time is believed to be required; however, in the event an additional fee or extension of time is required, please charge such fee or extension of time requested to the IBM Deposit Account 50-0563.

Respectfully submitted,

Antony P. Ng
Registration No. 43,427
DILLON & YUDELL, LLP
8911 N. Cap. of Texas Hwy., Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPELLANTS